Business & Society
1–29
© The Author(s) 2017
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/0007650317717957
journals.sagepub.com/home/bas

The (In)effectiveness of Voluntarily Produced Transparency Reports

Christopher Parsons[1]

Abstract

This article analyzes the relative effectiveness and limitations of companies' voluntarily produced transparency reports in promoting change in firm and government behavior. Such reports are published by telecommunications companies and disclose how often and on what grounds government agencies compel customer data from these companies. These reports expose corporate behaviors while lifting the veil of governmental secrecy surrounding these kinds of compulsions. Fung, Graham, and Weil's "targeted transparency" model is used to evaluate the extent to which these reports affect behavior. From the analysis, it is evident that telecommunications companies' transparency reports are only partially effective; while firms may modify their reports to present more information, these reports do not necessarily induce government to more broadly reveal its own activities. The article ultimately suggests that voluntarily produced transparency reports may become more comparable with one another as a result of either corporate reports evolving in consultation with external stakeholders or following a crisis that prompts government or industry to adopt a given standard. Such standards may positively influence the effectiveness of reports while concealing as much about firm behaviors as they purport to reveal.

[1]University of Toronto, Ontario, Canada

Corresponding Author:
Christopher Parsons, Citizen Lab, Munk School of Global Affairs, University of Toronto, At the Observatory, Third Floor, 315 Bloor Street West, Toronto, Ontario, Canada M5S 0A7.
Email: christopher@christopher-parsons.com

Keywords
corporate transparency, Internet reporting, politics, standardization, telecommunications

Governments have long requested information from intermediaries, such as telegraph and phone companies (Chan & Camp, 2002; Landau, 2010). But only recently have some intermediaries begun collating and publishing the number of such requests they receive each year and the extents to which they provide responsive information to the requests (Losey, 2015; Micek, 2016; Parsons, 2015a). Intermediaries call such publications "transparency reports." They are produced, in part, because governments do not publicly disclose all the kinds of lawful surveillance that they engage in or the regularity at which such activity is undertaken (Landau, 2010; Molnar, Parsons, & Zoave, 2017; Parsons & Israel, 2016; Soghoian, 2012).

Transparency reporting projects of this type are centrally focused around collating and disclosing information (Eigffinger & Geraats, 2006) to establish the "availability of firm-specific information to those outside the firm" (Bushman, Piotroski, & Smith, 2004, p. 207). This mode of reporting can operate as either "a form of verifiability" or as a kind of performance that is associated with some corporate social responsibility (CSR) efforts (Albu & Flyverbom, 2016) that are ostensibly meant to provide "information on matters of public concern" (Cotterrell, 1999, p. 414). Although such information may lift the veil of corporate secrecy by exposing otherwise hidden compliance with government requests (Davis, 1998), doing so simultaneously lifts the veil of *government* secrecy.

The action of exposing activities that governments have chosen to keep hidden from public view, and publishing information in excess of that provided by government, leads telecommunications companies' transparency reports to adopt a political character by filling an information disclosure gap left by government (Scherer & Palazzo, 2011). The exposure of government agencies' access to intermediary information assumes a heightened political importance given the volume of information mobilized as well as the number of services offered by telecommunications intermediaries and which pervade daily private and public life (Deibert, 2013; DeNardis, 2014; Hildebrant, 2015; MacKinnon, 2012). The political potential for these reports are further amplified when considered against the backdrop of revelations concerning state-driven mass and bulk monitoring of telecommunications traffic (Clement & Obar, 2015a), as well as the expansion of government powers to compel information from information intermediaries (Parsons, 2015a) and absence of countervailing accountability of how such powers are used.

Government agencies are now recognized as adopting novel interpretations of law (Freeze, 2016; Molnar et al., 2017) or exploiting ambiguities in law itself (Israel, 2015; Molnar & Parsons, 2015) to justify the aforementioned contemporary modes of intruding into private life. Telecommunications companies' publication of transparency reports can potentially provide at least some detail about the extent to which citizens' private lives are intruded upon by their governments, but such reports must be critically interrogated on the basis that transparency projects can produce "new dimensions of opacity and obscurity" (Hansen, Christensen, & Flyverbom, 2015). This article examines the rise of telecommunications transparency reports to assess the extent to which disclosing information about lawful government surveillance can prompt changes in firm or governmental behavior, as well as to consider what such reports may reveal and leave hidden.

The "Transparency and Accountability" section examines the intersection of transparency reporting, CSR, and accountability. Recognizing transparency as a contested concept, it ultimately draws upon Fung, Graham, and Weil's (2007) model of "targeted transparency" to subsequently evaluate the extent to which telecommunications companies' transparency reports are effective in encouraging behavioral changes in firms and government. The "Canadian Telecommunications Transparency Reports" section presents Canadian companies' reports for a case study analysis based on the underlying political stability that preceded their release. It subsequently describes the content of those companies' reports. The "Effectiveness Targeted Telecommunications Transparency Reports" section evaluates the extent to which these reports constitute "targeted transparency reports" and their effectiveness in prompting behavioral changes. The "Standardization and Maturation of Transparency Projects" section tentatively discusses how, and on what basis, these currently voluntary reports might be standardized by firms over time and how such standardization may selectively reveal and hide aspects of corporate involvement with government requests. The "Conclusion" section summarizes the article's arguments and poses lines of future research.

Transparency and Accountability

Where firms act transparently, they collate and present, data (Eigffinger & Geraats, 2006) to establish the "availability of firm-specific information to those outside the firm" (Bushman et al., 2004, p. 207) to potentially provide "information on matters of public concern" (Cotterrell, 1999, p. 414). Information that is provided, however, does not necessarily clarify a firm's behavior. Hansen et al. (2015) recognize that transparency is conceptually paradoxical insofar as it "produces new dimensions of opacity and obscurity." As a result, scholars are advised to pay "careful attention to the human and material operations that go into the production of transparency" (Hansen et al., 2015). In a separate analysis, Albu and Flyverbom (2016) develop a framework to differentiate verifiability and performativity approaches to transparency. Verifiable approaches focus "on how information is disclosed to verify a particular state of affairs," whereas performativity approaches "are less certain that more information generates better conduct" (Albu & Flyverbom, 2016, p. 13). The limitations of transparency are also taken up by Johnson and Regan (2014), who argue that transparency can function as a house of mirrors that distorts, extends, and distends information based on what is revealed, by whom, when, and for what purpose. Thus, although the practice of being transparent "is generally understood to refer to practices in which organizations (and sometimes individuals) reveal information about their behaviour," the fact that such revelations are sometimes linked to an organization controlling its public image means that scholars should take into account the fact that "the organizations or individuals have some control over the information that they disclose" (Wayland, Armengol, & Johnson, 2012, p. 243).

Given the distorted potentials for released information, such releases may not correct information asymmetries, promote intended policy changes, or lead to alterations of behavior. Emergent from their assessment of the literature, Albu and Flyverbom (2016) argue that studies of transparency focusing exclusively on providing information "gives primary attention to whether transparency efforts contain accurate and sufficient information to serve the purpose of providing clarity, predictability, and understandability" (p. 16). In contrast, transparency studies attentive to performativity are mindful of the human subject's ability to decode communicated information and the communicative processes that are involved in making information intelligible to a real—as opposed to imaginary or idealized—public.

The communication of information from firms to their stakeholders is oftentimes intermediated by third-party experts or the media (Licht, 2014; Sauder & Lancaster, 2006). Some of the stakeholders targeted by communications can include those interested in environmental, social, and financial issues (Belal, 2002; Chiu, 2010; Gray, 2007; Owen & O'Dwyer, 2008; van der Laan Smith, Adhikari, & Tondkar, 2005; Villiers, 2006). However, the attention of the intended stakeholders of any transparency project can be episodic, meaning that these stakeholders may not always be effective at intermediating information between a firm and the broader public. Such potential for inattention to disclosures by stakeholders can occur because

> the crowdsourcing enabled by transparency is not evenhanded, unbiased, consistent, or itself accountable. The "crowd" that watches consists of those who are intensely interested in whatever is being watched and often shares a certain perspective. The crowd also tends to be episodic in its coverage. (Regan & Johnson, 2014, p. 166)

The episodic attention of the crowd of stakeholders can explain why firms may be incentivized to routinely publish CSR documents as part of their efforts to generate monetary and nonmonetary benefits from such activities (Schaltegger & Wagner, 2006; Tetrault Sirsly & Lvina, 2016). This routine means that when the crowd examines an organization's activities it will be presented with information to grapple with and assimilate, as opposed to lacking information and arriving at imagined reasons for an organization's lack of transparency into its activities. Such episodic attention may also give further reason for firms to monitor who is reading and intermediating firm-released data so as to ensure that the firm's intended interpretations are being received and communicated (Barnett & Leih, 2016): Firms want to ensure that the material and symbolic resources invested in rendering their activities transparent is generating the anticipated benefits. Firms also engage in such monitoring for strategic purposes, such as evaluating whether released information is either enhancing attention to low-visibility firms or maintaining or accentuating the status of high-visibility CSR firms (Tetrault Sirsly & Lvina, 2016). Firms engaged in novel types of reporting may be particularly sensitive to how their publications are received, such as when they stretch the concept of CSR to encapsulate political activities. Such political activities can entail companies compensating for "the gaps in national governance by voluntarily contributing to self-regulation and by producing public goods that are not delivered by governments" (Scherer & Palazzo, 2011, p. 903). In filling these gaps, companies can impose a degree of accountability upon government, insofar as by providing information "the public" can pose questions and pass judgment by way of elections or political actions, thus imposing consequences on legislative representatives or government agencies as a result of these agencies' own actions (Bovens, 2007).

One of the newest forms of transparency reporting involves telecommunications companies compensating for gaps in the national governance of governmental surveillance activities. Though there are a range of mechanisms to evaluate CSR reports that are issued by companies (Chen & Bouvain, 2009; Lopatta, Buchholz, & Kaspereit, 2016; Pava & Krausz, 1997; Pérez & del Bosque, 2013), these telecommunications transparency reports serve to fill a gap left by government and thus require a novel way of evaluating their contents. Telecommunications companies' reports parallel other forms of CSR reporting, insofar as they disclose firm behavior, while also having the effect of exposing lawful activities that were undertaken in relative secrecy at the behest or compulsion of state agents. This act of exposure could potentially overcome knowledge asymmetries among key stakeholders attentive to telecommunications surveillance activities and, in the resulting reactions and usage of the information, prompt changes in firm or government behavior. This dual potential outcome causes telecommunications transparency reports to extend beyond reporting focused on either compliance with mandatory government rules or self-reporting on behaviors fully or largely controlled by the firm (Chiu, 2010). Ultimately, these types of reports are intended to foster transparency around corporate activities and behaviors as well as hold government to some account for its agencies' use of their lawful powers.

Fung and colleagues' (2007) targeted transparency model lends itself to examining these types of telecommunications transparency reporting. Targeted transparency reports aim "to influence specific choices" by providing "information that is complex and factual" and encouraging "users to make reasoned judgements of their own" (Fung et al., 2007, p. 39). Targeted transparency policies are meant to reduce "specific risks or improve particular aspects of public services" and require "that government agencies, companies, and other private-sector organizations collect, standardize, and release factual information to inform public choices" (Fung et al., 2007, p. 28). In filling a governmental policy gap, telecommunications companies' reports are ostensibly designed to present information to influence specific choices by consumers and citizens.

Mature targeted transparency policies are often borne from crises, such as those pertaining to environmental or financial issues, and typically possess five design features. First, the policy or report should be designed to accomplish a specific policy purpose. These purposes can vary widely and extend beyond simply correcting an information asymmetry. Such corrections can be made so as to significantly reduce the risks to the public, when a lack of information can impair the quality of critical services provided to stakeholders, when the asymmetry perpetuates "unacceptable patterns of discrimination or other social inequities," or when the asymmetry allows "corruption to persist in important institutions that serve the public" (Fung et al., 2007, pp. 40-41).

Second, the policy or report should have specified disclosure targets: Organizations should only be compelled to disclose information when they are clearly associated with the policy problem the transparency initiative is intended to alleviate. If a policy is meant to address the release of heavy metals into a river, as an example, it would best be targeted toward the classes of firms that might be engaged in such activities. However, targeted transparency policies do not typically define the intended information users (Fung et al., 2007, p. 42). This leaves open who, specifically, will actually take up or intermediate the disclosed information.

Third, the disclosure must possess a defined scope of information. In some cases, this will involve releasing information that an organization normally retains for its own purposes, such as when firms are compelled to disclose how much steel they purchase from different countries for use in manufactured products. In other cases, firms will have to establish new systems of monitoring, measuring, review, and reporting. Where disclosing parties are resistant to implementing targeted transparency policies, they may try to limit the scope of what is disclosed as a kind of “second line of defense once the political will to require the disclosure has become clear” (Fung et al., 2007, p. 43).

Fourth, a transparency policy or report must include a defined information structure and vehicle. Such a framework “always specifies metrics, frequency of disclosure, and a communication vehicle” (Fung et al., 2007, p. 43) so that disclosed information is comparable across organizations that are compelled to release information. If metrics are not carefully established, then shifts in how something is measured can indicate changes in state even though there is no actual difference in what is being measured. This information needs to be provided to the stakeholders with sufficient regularity so as to reflect potential changes in the policy condition (e.g., release of quarterly financial statements to indicate changes in corporate health) and in a way that is understandable to stakeholders. If a policy is meant to help all customers eat better, as an example, the communications medium has to be sufficiently accessible that it does not require specialized educational criteria to use or act on the disclosed information.

Fifth, there should be some sort of an enforcement mechanism. It is essential to monitor “nonreporting or misreporting” firms and levy “penalties for those who violate disclosure requirements” so that disclosing firms assess the costs of noncompliance as higher than those with compliance (Fung et al., 2007, p. 45). Such penalties can include financial costs or, alternately, social costs that negatively affect either the reputation of the firm or any directors who are ultimately responsible for developing and issuing such reports (J. A. Brown, Buchholtz, Butts, & Ward, 2016).

Even if transparency reports possess each the aforementioned characteristics of targeted transparency reports, they are not necessarily effective. An effective report is characterized as “significantly advancing policy aims” linked with the transparency project (Fung et al., 2007, p. 54). The information in such reports must be sufficiently valuable that stakeholders are willing to invest their time and energy in integrating the information into their decision-making process and be compatible with how people process such information (Fung et al., 2007, pp. 55-59). As a result, reports that are intended to replace a government function or shed light on a function ought to adopt a presentation style that prompts integration or evaluation of firm-released data. The information must also be comprehensible; it must be presented in a way that lets stakeholders relate to it in the challenges that they face (Fung et al., 2007, p. 59). However, a targeted transparency report is not necessarily effective when the presentation of information is designed to advance a policy aim, is integrated into stakeholders' decision-making process, is comprehensible, and causes a change in behavior among stakeholders. Information disclosers must, themselves, also change their decisions and actions following the behaviors exhibited by stakeholders. As noted by Fung and colleagues (2007), "[w]hen disclosers incorporate user responses to information in their decision calculus, we say that new information has become embedded in disclosure decision-making processes. Highly effective transparency policies, then, are doubly embedded" (p. 65).

Targeted transparency projects can be measured as being either highly effective, moderately effective, or ineffective (Fung et al., 2007, pp. 74-77). Highly effective policies significantly change the behavior of users of information as well as disclosers of information in the course of advancing the intended public policy. Moderately effective policies change the "behaviour or a substantial portion of users and disclosers in the intended direction" while leaving "gaps in behaviour change" and simultaneously producing "unintended consequences" (Fung et al., 2007, p. 77). Ineffective policies do not appreciably change the behaviors of users or disclosures, or behavior changes are different from those intended.

In summary, telecommunications transparency reports functionally expand the range of issues typically captured by corporate responsibility because they involve companies at least partially assuming the state's responsibility to annually publish information concerning lawful government surveillance activities. By applying the model of targeted transparency reporting, it is possible to ascertain whether companies have developed reports that are structured to reduce specific risks or improve particular aspects of public services and evaluate whether the reports which are being issued are highly, moderately, or not effective in their goals of advancing policy debates concerning governmental access to corporate data. Effectiveness can be measured by analyzing whether the information presented could facilitate public policy aims and, second, whether those aims have manifested vis-à-vis shifts in either firm or government behaviors.

Canadian Telecommunications Transparency Reports

Private telecommunications intermediaries such as Google, AT&T, and Bell Canada enjoy privileged roles in the daily lives of citizens. Citizens "have come to depend on them to safeguard our information and private communications and to prevent that information from falling into the hands of third parties" (Kerr & Gilbert, 2004, p. 164). This situation gives the companies "power and discretion: power to control our online behaviour and discretion to alter our outcomes" (Kerr & Gilbert, 2004, pp. 164-165). While scholars continue to debate the influence and power associated with intermediaries to stymie or promote certain kinds of speech and association (Dann & Haddow, 2008; Rosen, 2011; Ruan, Knockel, Ng, & Crete-Nishihata, 2016; Sartor & Cunha, 2010; Senft, Ng, Knockel, & Crete-Nishihata, 2015), the influence of intermediaries on establishing default mechanisms by which people communicate (Knockel, Senft, & Deibert, 2016; Schneider, 2016; Soghoian, 2010), or the privacy implications of corporate activities (Ahmed, 2017; Ahmed & Fung, 2017; Bennett, Parsons, & Molnar, 2014; Deibert, 2013), there has been less attention given to companies' publications of government agency requests for access to data processed, transited, or stored by private intermediaries. Such publications could potentially clarify how governments exercise their lawful powers to intrude into citizens' private lives and fill the gap of governments declining to annually report such information, or even prompt governments to issue their own annual reports to clarify their actual activities.

Google was the first company to release a transparency report in 2010 (Schroeder, 2010). Other American companies were initially slow to follow Google in issuing similar types of reports and only began issuing them en masse following some of Edward Snowden's national security revelations (Greenwald, 2014). Post-Snowden, the reports were intended to encourage governments to strike a balance between privacy, security, and democratic principles. Facebook, in the blog post that accompanied its first transparency report in 2013, wrote,

> Government transparency and public safety are not mutually exclusive ideals. Each can exist simultaneously in free and open societies, and they help make us stronger. We strongly encourage all governments to provide greater transparency about their efforts aimed at keeping the public safe, and we will continue to be aggressive advocates for greater disclosure. (Stretch, 2013)

Similarly, Microsoft's post that was published alongside its first transparency report noted there had "been a broadening public interest in how often law enforcement agencies request consumer data from technology companies and how our industry responds to these requests" (Smith, 2013). Yahoo! wrote that "[d]emocracy demands accountability, and accountability requires transparency. We hope our report encourages governments around the world to more openly share information about the requests they make for users' information" (Bell, 2013). Many of the reports, such as those from Microsoft, Yahoo!, and Google, included detailed explanations of how the companies responded to lawful requests for data from government agencies. Moreover, a group of leading technology companies released an open letter to the U.S. government calling for reforms to national security laws (AOL et al., 2013) that were seen as threatening their business opportunities within and beyond the borders of the United States (Wyatt & Miller, 2013). In aggregate, the transparency reports issued by American companies were at least partially motivated to reassure national and international subscribers that the companies had rigorous processes for evaluating government requests for data, shed light on the regularity and breadth of such requests, and encourage reforms in government surveillance activities.

In contrast to American companies, a multiyear effort by Canadian journalists, academics, and independent officers of Parliament to learn how many wiretaps (i.e., live interceptions of communications between persons), pen register/trap trace orders (i.e., live interceptions of numbers dialed to, and from, selected telephone numbers), and disclosures of subscriber data that were occurring annually (Braga, 2014; Gowlings, 2011; Office of the Privacy Commissioner of Canada, 2014) preceded Canadian companies' decision to release transparency reports. Canadian governments are only required to publicly report on their use of wiretaps (Koutros & Demers, 2013), and not on their use of other kinds of lawful surveillance techniques such as impersonating cellular towers, compelling intermediaries to produce retained data, compelling or requesting intermediaries to disclose subscriber- and billing-related information, or using malware to intrude into suspects' computers (Deibert, 2013; Molnar et al., 2017; Parsons, 2015a; Parsons & Israel, 2016).

The Citizen Lab, a research laboratory at the Munk School of Global Affairs at the University of Toronto, and workplace of the author, sought to persuade companies to release these reports over the course of 2014. Companies were sent public letters requesting detailed information about their data handling, management, and disclosure policies (Parsons, 2014b), responses were publicly analyzed (Parsons, 2014a) and reported on by the media (J. Brown, 2014; "CBC News," 2014), and a tool was developed to help individual subscribers pose data retention and disclosure to government agencies questions to their own telecommunications providers (Hilts & Parsons, 2015). These efforts were continuations of long-standing efforts to understand Canadian intermediaries' data disclosures (Parsons, 2015b). The reports that companies subsequently produced were not in response to a crisis such as evidence that they had disclosed bulk data to national security or policing agencies or shared data unlawfully with government agencies. The reports were, instead, issued to the surprise of government employees, academics, and journalists alike. In effect, whereas American companies were generally reacting to a sudden focusing event (Birkland, 2007)—the Snowden disclosures—the Canadian situation lacked a sudden revelation of facts that forced firms to collectively react to changes in the media, public, and policy agendas (Birkland, 2007; Critcher, 2002; McCombs, 2004).

The different political and policy situations experienced by American and Canadian companies were important. Most American intermediaries faced a direct, and very public, series of facts that threatened their ability to retain and gain subscribers both within and outside of the United States. The high degrees of variability between and across firms' reports can be linked to the emergency nature of their respective reports' development and release: Firms did not have time to carefully develop policy documents, work across industry lines to develop consensus on the most important details to publicize, or work with external stakeholders to ensure that the released data would be useful in understanding corporate and governmental activities. They were also released contra to government interests, and thus were not required to conform to government-sanctioned reporting standards. In contrast, Canadian companies had the opportunity to more carefully, and deliberately, create and publish their own transparency reports. They could communicate across firms as well as with external stakeholders to develop agreed-upon ways of collating and publishing data. This variation in situations opened the possibility for Canadian reports to be differentiated from those of American intermediaries, which are often noncomparable and provide variable utility in understanding firm behavior to government requests for customers' data (Losey, 2015). All major Canadian telecommunications companies also predominantly operate within the geographic boundaries of Canada; the dominant companies function as an oligopoly that is highly resistant to international competitors entering Canada and these companies do not have subsidiaries or offer services in other countries. This geographic isolation means that evaluating whether the Canadian government's behaviors change following the release of corporate transparency reports involves only examining a single government, whereas analyzing the effects of multinationals' reports could involve comprehensive examinations of government reactions around the world. Analyzing Canadian companies' reports is, then, a more contained exercise than analyses of many American companies that operate internationally and which have released transparency reports.

To analyze Canadian companies' transparency reports, they were comprehensively collected on June 1, 2015. Companies that had released such reports included Rogers, TELUS, SaskTel, Wind Mobile, and MTS Allstream. TekSavvy, rather than release a formal report, responded to questions posed to it by the Citizen Lab in 2014. Each of the companies committed to releasing annual reports. Only TekSavvy failed to release its 2015 report. Whereas several of Canada's largest telecommunications providers, such as Rogers and TELUS, had published transparency reports, many other companies had not. Companies that had not produced a report included but was not limited to Bell Sympatico (national telecommunications provider), Shaw Communications (regional telecommunications provider), Videotron (regional telecommunications carrier), and Bell Aliant (regional telecommunications carrier).

In 2014, Rogers received 20,438 requests for customer names and addresses, 71,501 requests for data under court order or warrant, 2,315 requests based on government exercising statutory powers, 10,016 requests based on exigent or emergency circumstances, 384 requests meant to respond to child exploitation emergencies, and one request pursuant to Mutual Legal Assistance Treaties (MLATs). The report noted that the company refused or provided no customer information in 2,278 cases (Rogers Communications, 2015). TELUS published that it had responded to 3,550 court orders and 453 subpoenas, 30,946 requests for subscriber names or address information, 1,247 requests based on government exercising existing statutory powers, 61,598 emergency calls (such as when authorities request information to locate or assist persons where their life, health, or security is at risk), and 144 requests pursuant to child exploitation emergency requests, and two requests pursuant to MLATs (TELUS, 2015). TELUS, like Rogers, did not record the number of subscribers or accounts affected by requests from government agencies.

SaskTel is a regional telecommunications provider. It received fewer requests for information than Rogers or TELUS, with most to "confirm a customer's current name and address." SaskTel's transparency report showed there were 889 requests for customer name and lookup information, 69 court orders that led the company to disclosing information related to 5,447 persons, 949 freedom of information and protection of privacy requests, 185 federal or provincial government formal demands, 4,616 emergency requests, and 31 requests related to child sexual exploitation. The company refused 61 requests over the year and did not identify the categories to which the denials were linked (SaskTel, 2015). Another smaller company, WIND Mobile (2015), published that it received 14,296 lawful access requests in its 2014 transparency report. 3,485 of those requests were for customer name and address information, 7,822 were associated with emergency response requests, and 2,989 were linked to court-ordered or legislative demands.

TekSavvy, differing from the other carriers, provided comprehensive responses to a public letter. In 2012 and 2013, combined, it received 52 requests from law enforcement agencies trying to correlate Internet Protocol (IP) addresses with subscriber names and related subscriber information. The company listed the data fields that were returned to requesting agencies, that the information was requested retroactively, and that only one of the 52 requests was made subject to a court order. Moreover, the company provided information in 17 cases and denied the remaining 35. And unlike any other company, TekSavvy differentiated between how many requests were made by federal (37%), provincial (10%), and municipal (54%) agencies. TekSavvy also outlined the kinds of data it retained in the course of providing telecommunications services to its subscribers, the retention periods for data that were collected, and that the company's "general legal standard is to require that government agencies provide a warrant, provide a production order, or demonstrate that obtaining one is justified but unfeasible due to exigent circumstances" (TekSavvy, 2014).

The mere release of Canadian companies' reports, even if they are meant to shed light on government activities as well as corporate responses, do not automatically meet the criteria of constituting targeted transparency efforts nor of being effective. We now turn to assess the extent to which these are actually targeted toward filling a gap left by government in reporting its surveillance activities and the extent to which they are effective in prompting behavioral changes.

Effectiveness Targeted Telecommunications Transparency Reports

Fully maturated targeted transparency reports must be designed for a specific policy purpose and those issued by telecommunications companies are designed to disclose how often, and on what grounds, companies are compelled to share information with government agencies. The failure of governments to release such information constitutes a social inequity on the grounds that it hinders parliament and the citizenry more broadly from holding the government to account for intrusions into private life (Korff, Wagner, Powles, Avila, & Buermeyer, 2017). The information asymmetry also prevents stakeholders from evaluating whether government agencies are unduly using their powers, or ensuring that uses of collected information are adequately explained in the courts (Israel & Parsons, 2016). That Canadian companies' reports are designed to respond to this public policy issue fulfills the first condition of a targeted transparency report.

The Canadian telecommunications industry's transparency reports followed from external stakeholders calling for details concerning the regularity and rationale of government access to telecommunications data. Only the kinds of firms that were likely receptors of governments' orders for such data have released transparency reports, as opposed to noninformation services companies that might also receive requests by government for customer information. Though the reports followed from external pressures, they were not explicitly written for any given audience; companies blandly stated that the reports followed from the interest some customers expressed in privacy-related issues (Rogers Communications, 2015; TekSavvy, 2014). Combined, that only certain classes of organizations are publishing data without explicitly identifying the stakeholders the reports are for, meets the second condition of a targeted transparency report.

Companies' reports were exclusively focused on the regularity at which the companies disclose information to government agencies. Given that external stakeholders had called for companies to make public information concerning companies' disclosure of information to government agencies, and that all the information disclosed pertains to such activities, the scope of information provided does broadly correspond to stakeholder calls, thus satisfying the third criteria of targeted transparency reporting. However, the failure to publicly release information concerning the policies that firms use to evaluate requests issued by government may reveal firms' resistance or hesitation to disclosing all aspects of the process of compelling information about their subscribers.

Although the scope for telecommunications transparency reports is relatively defined, the structuration of the disclosed information runs counter to that adopted in mature and effective targeted transparency models. Canadian companies, as noted previously, have adopted competing reporting formats despite having had the option to develop and release cross-comparable reports in the absence of a political crisis. Furthermore, the actual data that they published often fails to explain why information was disclosed or the extent to which companies' subscriber bases are affected. All companies that released a formal report in Canada continue to release them on an annual basis, with the exception of TekSavvy, though that company has only ever responded to external questions as opposed to issuing a formal report. As a result, while the formal reports are being regularly issued by firms that are taking part in the practice of reporting, the information that is presented limits how intermediating parties can evaluate or explain government requests for customer-related data. This limitation follows from external parties being unable to ascertain the regularity at which specific powers or orders are used to compel information from telecommunications companies or the breadth of such orders.

Whereas government agencies or independent bodies are typically expected to exercise enforcement powers to ensure firms comply with the terms of issuing targeted transparency reports, it has been intermediaries, such as nongovernmental organizations (NGOs), academics, and the press that have noted whether, and when, companies' reports are due (Chung, 2015, 2016; Clement & Obar, 2014, 2015b). These same parties are responsible for analyzing the contents of reports and the significance of what was or was not disclosed. Although TekSavvy has not experienced a public penalization for its failing to issue annual reports—no media organization has commented on the company's failure to produce formal reports—some of this may be linked to its marginal market share relative to incumbent Canadian telecommunications companies along with the company's litigation in defense of its subscribers' privacy (Sehra, 2016) and defense of customer privacy interests in government consultations (TekSavvy, 2016). In the absence of an effort to penalize the company, however, it remains uncertain whether such disciplinary actions would affect a firm's willingness to produce annual reports after having previously committed to doing so. Where journalists have noted that companies are not releasing reports, such as Bell Canada, the only effect has been Bell's unwillingness to even comment on the company's decision. Thus, while the utility of the enforcement mechanisms is unclear when it comes to firms that are releasing reports, media reports have not encouraged additional firms to release reports when they have been directly asked about releasing them.

The aggregate effectiveness of reports is gauged by Fung and colleagues (2007) based on whether the reports in question advance a policy position, present information in a way that is comprehensible and useful to stakeholders, and prompt changes in disclosers' habits following their issuance. In addition to, and beyond, these characteristics, the effectiveness of the reports can be gauged on whether they effect change in government: Do these reports lead to modifications in government behavior by leading to greater revelation of government agencies' access to data held by telecommunications companies?

Reports have proven useful to some scholarly analyses of telecommunications surveillance practices in Canada, and fueled greater understanding of the scope of government access to telecommunications data (Clement & Obar, 2014, 2015b; Parsons, 2015a). As evidenced from the listing of categories denoted in companies' transparency reports, the Canadian industry has not settled on a common standard for categorizing different kinds of requests that its members receive from government agencies. Further complicating matters, by not differentiating between the specific laws that are called upon to make these requests, a reader cannot determine which agencies are interested in the data, which laws are used to authorize the requests, or what kinds of data agencies might be requesting. Moreover, only a minority of companies attempt to clarify how many subscribers are affected by given requests. The result is that readers often cannot determine if each order tends to affect one, two, 10, or 10,000 persons; in Canada, a single order can affect tens of thousands of subscribers (e.g., *R. v. Rogers Communications & Telus Communications Company, 2016 ONSC 70*, 2016). Furthermore, few companies explain whether they refused certain requests and, if so, which requests they denied. Nor is it always clear *why* a given set of requests were declined: In the case of Rogers, as an example, the company refuses requests when its legal team finds that there is no responsive data to the request *or* because the company believes the request is overbroad and needs to be reframed. The reports do reveal some facets of corporate behavior—the numbers of requests and disclosures—while concealing the specific powers used to compel information, numbers of persons specifically affected, or particular corporate policies in responding to government requests. As a result, the reports actually have the effect of keeping secret important aspects of government requests for telecommunications data and consequently only provide a modicum of transparency of corporate activity.

Despite the aforementioned limitations, telecommunications companies' transparency reports are routinely taken up by the press—which regards the information as sufficiently useful to report on each year—as well as by scholars who annually evaluate the privacy practices of telecommunications companies (Clement & Obar, 2014, 2015b). Companies, themselves, have also gradually evolved their own reports by adding new categories (e.g., Rogers Communications, 2015) that are influenced to some extent by meeting with stakeholders to determine what information should be introduced into future reports. The reports have also prompted the government of Canada to release a noncompulsory telecommunications transparency reporting format for private businesses (Industry Canada, 2015), and an independent officer of Parliament, the privacy commissioner of Canada, has repeatedly called for corporate transparency reporting to be compulsory (Office of the Privacy Commissioner of Canada, 2016). Though the government of Canada's reporting format was criticized for not being developed collaboratively with stakeholders external to government (Geist, 2015), it would, if adopted, lead companies to present more extensive information concerning the regularity at which government agencies make requests for telecommunications companies' data. The federal government of Canada has not, however, indicated that it would expand its own statutory reporting requirements concerning how government agencies collect, use, or retain data compelled from telecommunications companies.

By releasing telecommunications transparency reports, companies have successfully influenced the behavior of users, insofar as the reports are taken up by stakeholders who then intermediate the results to the public more broadly. This indicates that information as released today is sufficiently useful and comprehensible that it possesses some utility. Moreover, the behaviors of disclosers have also changed somewhat, insofar as additional categories of data have been included in some companies' reports. Although there has been a change in government behavior, it differs from that sought by academic, NGO, and corporate stakeholders. These stakeholders wanted the government to release additional data concerning its agencies' requests for personal information from telecommunications companies. Rather than commit to this degree of behavioral change, the government merely presented a voluntary reporting format that private companies could voluntarily adopt. When comparing these results against Fung and colleagues' (2007) tripartite division of effectiveness, then, Canadian companies' reports can be graded as being moderately effective: They changed the behavior of a substantial number of users and disclosers of information while leaving gaps in behavioral change and also produced an unintended effect, or consequence, on the part of government.

Standardization and Maturation of Transparency Projects

Canadian telecommunications companies have not issued their transparency reports in reaction to a crisis. As noted by Fung and colleagues (2007), fully maturated targeted transparency policies are often created as "serendipitous inventions that responded to perceived crises" (p. 28). Due to these crises, the resulting reporting is designed to address a delineated policy issue, require a specific group to disclose data, present a particular scope of information linked to the policy issue, possess an articulated way of structuring information and delivering it to external parties, and involve some preestablished enforcement mechanism. Voluntary reporting systems that become imbued with a mandatory disclosure regime and associated with nongovernmental enforcement mechanisms, in contrast to crisis-based reporting, tend to be evolutionary and subject to societal evaluation (Suchman, 1995). Such evolution can follow from discourse concerning the framing and structuration of how information is shared between stakeholders internal and external to the firm (Haack, Schoeneborn, & Wickert, 2010, 2012). As a result, the initial standards set as part of any given transparency project may constitute the beginning, as opposed to the end, of the standardization process itself (Haack et al., 2012, citing Ansari, Fiss, & Zajac, 2010). Thus, the present status of telecommunications transparency reporting is not necessarily representative of the end of a standardization process but instead potentially of an early stage in a longer process.

Standards development can involve parties actively engaging in dialogue with one another, during which they realize a socially shared reality that captures the emergent nature of the policy issue in question in tandem with the material and social needs of involved parties (Haack et al., 2012). In other words, as stakeholders come together and discuss their perceptions of the policy problem, possible solutions, and costs of action, they can produce "a gradual convergence of identities" (Haack et al., 2010, p. 12). By sharing in meaning-making, the stakeholders involved in the policy issue—which in the case of telecom transparency projects involves telecommunications companies, NGOs, and academics, as well as government—may come to a commonly understood position concerning the relative value of standardizing the information disclosed by firms as it pertains to advancing the policy issue at hand.

Such collaborative meaning-making does, in fact, take place through the publication of transparency-related reports and guidelines (Industry Canada, 2015; Parsons, 2015a, 2016; Woolery, Budish, & Bankston, 2016) and regular meeting of stakeholders at public and private forums. Such publications and meetings help to establish reporting as a kind of "lived" issue, though the absence of consensus concerning how to standardize the reporting can leave community members with contested conceptions of what, specifically, transparency is meant to solve and how it should do so. As a result, stakeholders may present sets of potential standards as a way to continue debate and leave open whether the shared meanings that are documented in reports and guidelines that attempt to integrate shared discourse by stakeholders can or will be adopted.

The standardization and voluntary adoption of transparency projects for other policy issues has often relied on NGOs or other actors being reputable *and* capable of inflicting reputational damage on organizations that are involved in nontransparent practices that affect social goods (Haack et al., 2010, 2012). In the case of international finance, standards were adopted to equalize risks across firms as well as to facilitate business operations (Fung et al., 2007; Haack et al., 2010). In the case of telecommunications reports, however, government is largely resistant to its behavior being disclosed. In other circumstances, such as those related to financial or environmental issues, governments are often involved in the development and enforcement of transparency projects and policies. When it came to financial transparency projects, government interests have often been at least somewhat aligned with greater transparency concerning capital movements, but this is less the case when it comes to transparency projects that are designed to disclose secretive government behaviors. However, government's nonenforcement of corporate telecommunications transparency standards could shift in the event of a focusing event.

Transparency reports could eventually be standardized following further meaning-making and collaboration between stakeholders invested in the issue or following a crisis taking place that is equivalent in caliber to the Snowden revelations. Should a crisis that revitalizes the problem of telecommunications transparency arise, the standards that have been proposed by government, NGOs, and academics might come to represent a solution to the problem being revealed (Kingdon, 2003). This process of developing standards that lay idle for the appropriate policy problem coheres with how other policy instruments are developed only to lay unused for years or decades (Sharp, 1994; Woods & Peake, 1998). Hence, the shared meaning-making that takes place to develop the standards now being proposed might functionally represent a solution to a problem, where the problem that led to the transparency reports in the first place has sufficiently retreated from the public agenda that there is currently no driving impetus to implement a reporting format that fully coheres with Fung and colleagues' (2007) model. The maturation of existing corporate transparency projects, then, may either take place following an evolutionary process of meaning-making or following the sudden shock of an unexpected focusing event or crisis.

There is a danger, however, that even if dialogue and meaning-making occur between stakeholders invested in a policy issue any standardization protocol may conceal as much as it reveals. Although standardization might establish a particularized flow of publicized information (Bushman et al., 2004, p. 207) following extensive dialogue and negotiation with stakeholders, the act of standardizing information can distort, extend, and distend what is presented (Johnson & Regan, 2014) if corporate or governmental stakeholders take advantage of standardization processes and negotiations to effectively obfuscate information that is as much, or more, important than that which is being publicized. In the case of telecommunications transparency reports, when companies report on how often and for what reasons governments request access to their data, they may not also discuss their involvement in coaching government agencies in how to legally compel such information in the first place (Morin, 2015; Seglins, 2016) or their proactive efforts which are designed to ensure that telecommunications services can be accessible to government agencies (Alcatel Lucent & Rogers Communications, 2012; Rogers Communications, 2014). By developing transparency reports that are focused on the regularity of requests instead of the reasons such requests take place, the process of being transparent may end up being suborned to an organization controlling its public image (Wayland et al., 2012) or focus on providing only certain kinds of verifiable information that are expected to enhance the organization's reputation. These possible limits on transparency reporting cohere with Chiu's warning that standardizing reports can result in "generic and nondescript reporting" that "allows corporations to primarily use the CSR report in pursuit of the business case" as well as "prematurely provide glib and overly-confident perceptions of what CSR performance is" (Chiu, 2010, p. 375). In short, the standardization of transparency reports that focus on the regularity and rationales of certain government-firm behaviors and not others may alleviate one type of information asymmetry while not publicizing information about what is responsible for the problem that the transparency reporting is meant to alleviate in the first place.

Conclusion

This article has analyzed the relative effectiveness of some telecommunications companies' transparency reports to understand the potentials and limitations of transparency reports to promote changes in firm and government behavior. These reports were designed to promote awareness in lawful government surveillance activity and were only partially effective. In the case study, though the reports have evolved in reaction to stakeholder responses, thus indicating a double embedding of the reports, the government has declined to more expansively disclose its own activities. The article ultimately suggested that standardization of voluntarily produced reports might follow from either the evolution of these reports in consultation with stakeholders who are involved in shared meaning-making or following the advent of a crisis. However, any standardization effort may conceal how firms themselves facilitate government intrusions into private life, such as by coaching governments on how to compel information from firms in the first place or by proactively designing their services to ensure they are accessible to government requests.

The case analysis focused on Canadian businesses based on their opportunities to learn from American companies' reports and abilities to develop, and release, their reports after potentially developing a common approach within their industry association and without the need to respond to a political crisis. Despite the opportunity to develop harmonized reporting protocols, no Canadian business has adopted the same reporting format as another industry competitor. As a result, future work could extend the same model of targeted transparency reporting to gauge the effectiveness of discordant reports in other jurisdictions to evaluate whether they are effective in changing firm behavior, as well as the behavior of the countries that the firms operate in. Such work could be nation-specific, such as focusing on companies that exclusively operate in a single nation, or evaluate how transnational companies' reports prompt behavioral changes in the firms, as well as whether and how they prompt multiple governments to change their own behaviors.

Future research might also focus on whether there are differences in how reports are developed following the initial release of reports to combat a crisis or following consistent pressure to issue them. Do firms engage with external stakeholders to adjust or modify reports differently based on the driving motivation for the reports? And do stakeholders from civil society or government tend to engage principally with firms in a single jurisdiction or across borders? Exploring these questions would reveal the extent to which meaning-making within a given policy community is developed internationally and perhaps give hints as to whether international collaboration in either crisis or noncrisis situations is more or less likely to lead to a standardization of reporting formats.

Government agencies will continue to turn to intermediaries in the course of their investigations. And intermediaries will be able to provide more and more data as daily life is increasingly digitized and linked with Internet-based communications. Until legislative assemblies begin to impose statutory reporting requirements that compel government agencies to report on how they use lawful powers to compel information from intermediaries, the public will remain reliant on the private sector's transparency reports to understand the contours of government surveillance activity. Scholarly analysis and critique of such reports, then, assumes a heightened importance: Not only do telecommunications companies' reports provide ways of learning how firms' CSR activities can become politicized by filling in a reporting and accountability gap previously filled by government, but also critique of existing reports has the potential of contributing to the meaning-making of such reports and thus influence the design and release of future reports.

Acknowledgments

The author would like to thank the editors and anonymous reviewers for their comments on earlier versions of this article, as well as the attendees of a paper workshop in Copenhagen, Denmark for their comments. He also thanks Christopher Prince, Peter Micek, Kevin Spafford, and John Wunderlich for their feedback, as well as comments received from participants at the Citizen Lab Summer Institute. Finally, he thanks the numerous and unamed members of government and employees of telecommunications companies for sharing their thoughts about government accountability and transparency reporting.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The author received funding support in the form of a grant from the Canadian Internet Registration Authority as well as a Social Science and Humanities Research Council Postdoctoral Fellowship.

References

Ahmed, S. (2017). *Cashless society, cached data: Security considerations for a Chinese social credit system*. Citizen Lab. Retrieved from https://citizenlab.org/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system/

Ahmed, S., & Fung, A. (2017). *Cashless society, cached data: Are mobile payment systems protecting Chinese citizens' data?* Citizen Lab. Retrieved from https://citizenlab.org/2017/01/cashless-society-cached-data-mobile-payment-systems-protecting-chinese-citizens-data/

Albu, O. B., & Flyverbom, M. (2016). Organizational transparency: Conceptualizations, conditions, and consequences. *Business & Society*. Advance online publication. doi:10.1177/0007650316659851

Alcatel Lucent & Rogers Communications. (2012, January 17-19). *Candidate LI solutions for MIKEY-IBAKE based on re-generation of random secret: Discussion and decision* (3GPP TSG-SA3LI, SA3#44LI). Barcelona, Spain.

Ansari, S. M., Fiss, P. C., & Zajac, E. J. (2010). Made to fit: How practices vary as they diffuse. *Academy of Management Review*, *35*, 67-92.

AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, & Yahoo! (2013, May 19). *Reform government surveillance*. Retrieved from https://www.reformgovernmentsurveillance.com/#may-19

Barnett, M. L., & Leih, S. (2016). Sorry to (not) burst your bubble: The influence of reputation rankings on perceptions of firms. *Business & Society*. Advance online publication. doi:10.1177/0007650316643919

Belal, A. R. (2002). Stakeholder accountability or stakeholder management: A review of UK firms' social and ethical accounting, auditing and reporting (SEA AR) practices. *Corporate Social Responsibility and Environmental Management*, *9*, 8-25.

Bell, R. (2013, September 6). *Sharing our first transparency report*. Yahoo! Retrieved from https://yahoo.tumblr.com/post/60456292987/sharing-our-first-transparency-report

Bennett, C., Parsons, C., & Molnar, A. (2014). Real and substantial connections: Enforcing Canadian privacy laws against American social networking companies. *Journal of Law, Information & Science*, *23*, 50-74.

Birkland, T. A. (2007). *After disaster: Agenda setting, public policy, and focusing events*. Washington, DC: Georgetown University Press.

Bovens, M. (2007). Analyzing and assessing accountability. *European Law Journal*, *13*, 447-468.

Braga, M. (2014, November 20). New documents show thousands of unreported wiretaps by Canadian cops. *Motherboard*. Retrieved from http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps-by-canadian-cops

Brown, J. (2014, May 6). Your telecom provider is selling your information to the government. *Canadaland*. Retrieved from http://www.canadalandshow.com/podcast/your-telecom-provider-selling-your-information-government/

Brown, J. A., Buchholtz, A., Butts, M. M., & Ward, A. J. (2016). Board socio-cognitive decision-making and task performance under heightened expectations of accountability. *Business & Society*. Advance online publication. doi:10.1177/0007650316675597

Bushman, R., Piotroski, J., & Smith, A. (2004). What determines corporate transparency? *Journal of Accounting Research*, *42*, 207-252.

CBC News. (2014, 30 April). Telecoms refuse to release information on private data given to feds. *CBC News*. Retrieved from http://www.cbc.ca/news/politics/telecoms-refuse-to-release-information-on-private-data-given-to-feds-1.2626286

Chan, S., & Camp, L. J. (2002, Summer). Law enforcement surveillance in the network society. *IEEE Technology and Society Magazine*, pp. 22-30.

Chen, S., & Bouvain, P. (2009). Is corporate responsibility converging? A comparison of corporate responsibility in the USA, UK, Australia, and Germany. *Journal of Business Ethics*, *87*, 299-317.

Chiu, I. H.-Y. (2010). Standardization in corporate social responsibility reporting and a universalist concept of CSR?—A path paved with good intentions. *Florida Journal of International Law*, *22*, 361-400.

Chung, E. (2015, April 9). Rogers transparency report shows fewer police requests for customer info. *CBC News*. Retrieved from http://www.cbc.ca/news/technology/rogers-transparency-report-shows-fewer-police-requests-for-customer-info-1.3026604

Chung, E. (2016, May 20). Rogers gave customer info to police, government in 97% of 2015 requests. *CBC News*. Retrieved from http://www.cbc.ca/news/technology/rogers-transparency-report-1.3591055

Clement, A., & Obar, J. (2014). *Keeping internet users in the know or in the dark: A report on the data privacy transparency of Canadian internet carriers*. IXMaps. Retrieved from https://www.ixmaps.ca/docs/DataPrivacyTransparencyofCanadianISPs-2013.pdf

Clement, A., & Obar, J. (2015a). Canadian internet "boomerang" traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges. In M. Geist (Ed.), *Law, privacy and surveillance in Canada in the post-Snowden era* (pp. 13-44). Ottawa, Ontario, Canada: Ottawa University Press.

Clement, A., & Obar, J. (2015b). *Keeping internet users in the know or in the dark: A report on the data privacy transparency of Canadian internet carriers*. IXMaps.

Retrieved from https://www.ixmaps.ca/docs/DataPrivacyTransparencyofCanadianCarriers-2014.pdf

Cotterrell, R. (1999). Transparency, mass media, ideology and community. *Journal for Cultural Research*, *3*, 414-426.

Critcher, C. (2002). Media, government, and moral panics: The politics of paedophilia in Britain 2000-1. *Journalism Studies*, *3*, 521-535.

Dann, G. E., & Haddow, N. (2008). Just doing business or doing just business: Google, Microsoft, Yahoo! and the business of censoring China's internet. *Journal of Business Ethics*, *79*, 219-234.

Davis, J. (1998). Access to and transmission of information: Position of the media. In V. Deckmyn & I. Thomson (Eds.), *Openness and transparency in the European Union* (pp. 121-126). Maastricht, The Netherlands: European Institute of Public Administration.

Deibert, R. (2013). *Black code: Inside the battle for cyberspace*. Toronto, Ontario, Canada: McClelland & Stewart.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Eigffinger, S. C. W., & Geraats, P. M. (2006). *Government transparency: Impacts and unintended consequences*. New York, NY: Palgrave Macmillan.

Freeze, C. (2016, November 3). In scathing ruling, Federal Court says CSIS bulk data collection illegal. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/news/national/in-scathing-ruling-federal-court-says-csis-bulk-data-collection-illegal/article32669448/

Fung, A., Graham, M., & Weil, D. (2007). *Full disclosure: The perils and promise of transparency*. New York, NY: Cambridge University Press.

Geist, M. (2015, July 7). *Why the new Canadian telecom transparency rules fall short*. Michael Geist (blog). Retrieved from http://www.michaelgeist.ca/2015/07/why-the-new-canadian-telecom-transparency-rules-fall-short/

Gowlings. (2011, December 11). *Re: Response to request for general information from Canadian Wireless Telecommunications Association (The "CWTA") Members*. Author. Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/let_140430/

Gray, R. (2007). Taking a long view on what we now know about social and environmental accountability and reporting. *Issues in Social and Environmental Accounting*, *1*, 169-198.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books.

Haack, P., Schoeneborn, D., & Wickert, C. (2010). *Exploring the constitutive conditions for a self-energizing effect of CSR standards: The case of the "Equator Principles"* (University of Zurich Institute of Organization and Administrative Science IOU Working Paper No, 115). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706267

Haack, P., Schoeneborn, D., & Wickert, C. (2012). Talking the talk, moral entrapment, creeping commitment? Exploring the narrative dynamics in corporate responsibility standardization. *Organization Studies*, *33*, 815-845.

Hansen, H. K., Christensen, L. T., & Flyverbom, M. (2015). Introduction: Logics of transparency in late modernity: Paradoxes, mediation and governance. *European Journal of Social Theory*, *18*, 117-131.

Hildebrant, A. (2015, April 10). Police asked Telcos for client data in over 80% of criminal probes. *CBC News*. Retrieved from http://www.cbc.ca/news/technology/police-asked-telcos-for-client-data-in-over-80-of-criminal-probes-1.3025055

Hilts, A., & Parsons, C. (2015, June 30-July 2). *Access my info: An application that helps people create legal requests for their personal information*. The 15th Privacy Enhancing Technologies Symposium, Philadelphia, PA.

Industry Canada. (2015). *Transparency reporting guidelines*. Government of Canada. Retrieved from http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html

Israel, T. (2015). Foreign intelligence in an inter-networked world: Time for a re-evaluation. In M. Geist (Ed.), *Law, privacy and surveillance in Canada in the post-Snowden era* (pp. 71-102). Ottawa, Ontario, Canada: Ottawa University Press.

Israel, T., & Parsons, C. (2016). *Written inquiry under Part 5 of the Freedom of Information & Protection of Privacy Act ("FIPPA") of British Columbia: In Re: Vancouver Police Department*. Office of the Information and Privacy Commissioner of British Columbia. Retrieved from https://cippic.ca/uploads/BCOIPC_F15-63155_ReVPD-OM-Intervention.pdf

Johnson, D. G., & Regan, P. M. (Eds.). (2014). *Transparency and surveillance as sociotechnical accountability: A house of mirrors*. New York, NY: Routledge.

Kerr, I., & Gilbert, D. (2004). The role of ISPs in the investigation of cybercrime. In T. Mendina & J. J. Britz (Eds.), *Information ethics in the electronic age: Current issues in Africa and the world* (pp. 163-172). Jefferson, NC: McFarland.

Kingdon, J. K. (2003). *Agendas, alternatives, and public policies (2nd ed.)*. Toronto, Ontario, Canada: Addison-Wesley Educational Publishers.

Knockel, J., Senft, A., & Deibert, R. (2016). *A tough nut to crack: A further look at privacy and security issues in UC browser*. Citizen Lab. Retrieved from https://citizenlab.org/2016/08/a-tough-nut-to-crack-look-privacy-and-security-issues-with-uc-browser/

Korff, D., Wagner, B., Powles, J., Avila, R., & Buermeyer, U. (2017). *Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes*. Social Sciences Research Network. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894490

Koutros, N., & Demers, J. (2013, March 15). *In Big Brother's shadow: Historical decline of electronic surveillance by Canadian federal law enforcement* (Working paper). Social Sciences Research Network. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220740

Landau, S. (2010). *Surveillance or security? The risks posed by new wiretapping technologies*. Cambridge, MA: MIT Press.

Licht, J. (2014). Transparency actually: How transparency affects public perception of political decision making. *European Political Science Review*, *6*, 309-330.

Lopatta, K., Buchholz, F., & Kaspereit, T. (2016). Asymmetric information and corporate social responsibility. *Business & Society*, *55*, 458-488.

Losey, J. (2015). Surveillance of communications: A legitimization crisis and the need for transparency. *International Journal of Communications*, *9*, 3450-3459.

MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom*. New York, NY: Basic Books.

McCombs, M. E. (2004). *Setting the agenda: The mass media and public opinion*. Cambridge, UK: Polity Press.

Micek, P. (2016, February 18). *Transparency Reporting Index*. Accessnow. Retrieved from https://www.accessnow.org/pages/transparency-reporting-index

Molnar, A., & Parsons, C. (2015). Unmanned aerial vehicles (UAVs) and law enforcement in Australia and Canada: Governance through "privacy" in an era of counter-law? In K. Walby, R. K. Lippert, I. Warren & D. Palmer (Eds.), *National security, surveillance, and emergencies: Canadian and Australian sovereignty compared* (pp. 225-248). New York, NY: Palgrave Macmillan.

Molnar, A., Parsons, C., & Zoave, E. (2017). Computer network operations and "rule-with-law" in Australia. *Internet Policy Review*, *6*(1). doi:10.14763/2017.1.453

Morin, S. (2015, April 15). *R v Spencer "lawful authority to obtain" (or not)* (2014 SCC 43). Canadian Legal Information Institute. Retrieved from http://canliiconnects.org/en/commentaries/36740

Office of the Privacy Commissioner of Canada. (2014). *Review of the Royal Canadian Mounted Police—Problems with statistics and identifying warrantless access files*. Author. Retrieved from http://cdn.michaelgeist.ca/wp-content/uploads/2015/03/rcmpauditmemo.pdf

Office of the Privacy Commissioner of Canada. (2016). *2015-2016 annual report to parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act*. Author. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/

Owen, D. L., & O'Dwyer, B. (2008). Corporate social responsibility: The reporting and assurance dimension. In A. Crane, D. Matten, A. McWilliams, J. Moon & D. S. Siegel (Eds.), *The Oxford handbook of corporate social responsibility* (pp. 384-409). Oxford, UK: Oxford University Press.

Parsons, C. (2014a, March 6). *The murky state of Canadian telecommunications surveillance*. Citizen Lab. Retrieved from https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/

Parsons, C. (2014b, January 22). *Towards transparency in Canadian telecommunications*. Citizen Lab. Retrieved from https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/

Parsons, C. (2015a). *The governance of telecommunications surveillance: How opaque and unaccountable practices and policies threaten Canadians*. Telecom Transparency Project. Retrieved from http://www.telecomtransparency.org/release-the-governance-of-telecommunications-surveillance/

Parsons, C. (2015b). Stuck on the agenda: Drawing lessons from the stagnation of "lawful access" legislation in Canada. In M. Geist (Ed.), *Law, privacy and surveillance in Canada in the Post-Snowden era* (pp. 257-284). Ottawa, Ontario, Canada: University of Ottawa Press.

Parsons, C. (2016). *Release: DIY transparency report tool*. Citizen Lab. Retrieved from https://citizenlab.org/2016/06/release-diy-transparency-report-tool/

Parsons, C., & Israel, I. (2016). *Gone opaque? An analysis of hypothetical IMSI catcher overuse in Canada* (Citizen Lab–Telecom Transparency Project // CIPPIC). Retrieved from https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf

Pava, M. L., & Krausz, J. (1997). Criteria for evaluating the legitimacy of corporate social responsibility. *Journal of Business Ethics*, *16*, 337-347.

Pérez, A., & del Bosque, I. R. (2013). Measuring CSR image: Three studies to develop and to validate a reliable measurement tool. *Journal of Business Ethics*, *118*, 265-286.

Regan, P. M., & Johnson, D. G. (2014). Policy options for reconfiguring the mirrors. In D. G. Johnson & P. M. Regan (Eds.), *Transparency and surveillance as sociotechnical accountability: A house of mirrors* (pp. 162-184). New York, NY: Routledge.

Rogers Communications. (2014, October 28-30). *Preservation discussion* (3GPP TSG-SA3LI, SA3LI #55). Portland, OR.

Rogers Communications. (2015). *Rogers Communications 2014 Transparency Report*. Author. Retrieved from http://www.rogers.com/consumer/privacy-crtc

Rosen, J. (2011). The deciders: The future of privacy and free speech in the age of Facebook and Google. *Fordham Law Review*, *80*, 1525-1538.

Ruan, L., Knockel, J., Ng, J. Q., & Crete-Nishihata, M. (2016). *One app, two systems: How WeChat uses one censorship policy in China and another internationally*. Citizen Lab. Retrieved from https://citizenlab.org/2016/11/wechat-china-censorship-one-app-two-systems/

R. v. Rogers Communications & Telus Communications Company, 2016 ONSC 70. (2016). Retrieved from https://ccla.org/cclanewsite/wp-content/uploads/2016/01/R-v.-Rogers-and-Telus-Judgment-January-14-2016-1.pdf

Sartor, G., & Cunha, M. V. d. A. (2010). The Italian Google-case: Privacy, freedom of speech and responsibility of providers for user-generated contents. *International Journal of Law and Information Technology*, *18*, 356-378.

SaskTel. (2015). *SaskTel 2014 Transparency Report*. Author. Retrieved from https://www.sasktel.com/wps/wcm/connect/a1a33ce6-ca5f-4077-ad67-44e9ebde3026/SkTel+Transparency+Report_Final+2014.pdf?MOD=AJPERES

Sauder, M., & Lancaster, R. (2006). Do rankings matter? The effects of. *U.S. News & World Report Rankings on the Admission Process of Law Schools*. *Law & Society Review*, *40*, 105-134.

Schaltegger, S., & Wagner, M. (Eds.). (2006). *Managing the business case for sustainability*. Sheffield, UK: Greenleaf.

Scherer, A. G., & Palazzo, G. (2011). The new political role of business in a globalized world: A review of a new perspective on CSE and its implications for the firm, governance, and democracy. *Journal of Management Studies*, *48*, 899-931.

Schneider, D. (2016, January). Don't expect encrypted e-mail in 2016. *IEEE Spectrum*, *2016*, 42-43.

Schroeder, S. (2010, September 21). Google fights censorship with transparency report. *Mashable*. Retrieved from http://mashable.com/2010/09/21/googles-transparency-report/#J.ygezK0i8qj

Seglins, D. (2016, December 15). Federal cabinet secretly approved Cold War wiretaps on anyone deemed “subversive,” historian finds. *CBC News*. Retrieved from http://www.cbc.ca/news/investigates/surveillance-cold-war-picnic-1.3897071

Sehra, A. (2016, January 12). The role of ISPs in Canada’s new copyright regime. *Slaw*. Retrieved from http://www.slaw.ca/2016/01/12/the-role-of-isps-in-canadas-new-copyright-regime/

Senft, A., Ng, J. Q., Knockel, J., & Crete-Nishihata, M. (2015). *Every rose has its thorn: Censorship and surveillance on social video platforms in China*. Citizen Lab. Retrieved from https://citizenlab.org/2015/08/every-rose-has-its-thorn/

Sharp, E. B. (1994). Paradoxes of national anti-drug policymaking. In D. A. Rochefort & R. W. Cobb (Eds.), *The politics of problem definition: Shaping the policy agenda* (pp. 98-116). Lawrence: University of Kansas.

Smith, B. (2013, March 21). Microsoft releases 2012 law enforcement requests report. *Microsoft*. Retrieved from https://web.archive.org/web/20130401072409/http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/03/20/microsoft-releases-2012-law-enforcement-requests-report.aspx

Soghoian, C. (2010). An end to privacy theatre: Exposing and discouraging corporate disclosure of user data to the government. *Minnesota Journal of Law, Science, & Technology*, *12*, 191-237.

Soghoian, C. (2012). *The spies we trust: Third party service providers and law enforcement surveillance* (Doctoral dissertation). Retrieved from http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf

Stretch, C. (2013). *Global government requests report*. Facebook. Retrieved from https://newsroom.fb.com/news/2013/08/global-government-requests-report/

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*, 571-610.

TekSavvy. (2014, June 4). *Re: January 20 data request (items 1-10); May 1 personal information template*. Author. Retrieved from https://citizenlab.org/wp-content/uploads/2014/06/TekSavvy-to-Citizenlab-2014-06-04.pdf

TekSavvy. (2016, December 15). *Re: Consultation on national security*. Author. Retrieved from https://www.documentcloud.org/documents/3243036-Consultation-on-National-Security-TekSavvy-2016.html

TELUS. (2015). *Sustainability Report 2015*. Author. Retrieved from https://telus-digital-sustainability-production.s3.amazonaws.com/uploads/2017/04/2015_Sustainability_Report-EN.pdf

Tetrault Sirsly, C., & Lvina, E. (2016). From doing good to looking even better: The dynamics of CSR and reputation. *Business & Society*. Advance online publication. doi:10.1177/0007650315627996

van der Laan Smith, J., Adhikari, A., & Tondkar, R. H. (2005). Exploring differences in social disclosures internationally: A stakeholder perspective. *Journal of Accounting and Public Policy*, *24*, 123-151.

Villiers, C. (2006). *Corporate reporting and company law*. Cambridge, UK: Cambridge University Press.

Wayland, K., Armengol, R., & Johnson, D. G. (2012). When transparency isn't transparent: Campaign finance disclosure and internet surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 239-254). New York, NY: Routledge.

WIND Mobile. (2015). *Wind Mobile Transparency Report 2014*. Author. Retrieved from http://www.windmobile.ca/docs/default-source/default-document-library/2014-transparency-report-wind-mobileABF7DF074C25.pdf

Woods, B. D., & Peake, J. S. (1998). The dynamics of foreign policy agenda-setting. *American Political Science Review*, *92*, 173-184.

Woolery, L., Budish, R., & Bankston, K. (2016). *The transparency reporting toolkit*. New America and The Berkman Center for the Internet & Society. Retrieved from https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Transparency.pdf

Wyatt, E., & Miller, C. C. (2013, December 9). Tech giants issue call for limits on government surveillance of users. *The New York Times*. Retrieved from http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html?pagewanted=all

Author Biography

Christopher Parsons (PhD, University of Victoria) is research associate and managing director of the Telecommunications Transparency Project at Citizen Lab at the Munk School of Global Affairs, University of Toronto. His research interests focus on surveillance, security, and privacy studies, and comparative public policy and regulation. His articles have appeared in such journals as *Canadian Journal of Law and Society*, *CTheory*, *European Journal of Law and Society*, *Information & Science*, *Internet Policy Review*, *Journal of Law*, and *Media and Communications*.